In 2020, the cybersecurity landscape was shaped by the challenges of scaling distributed IT environments and transitioning to work-from-home models during the pandemic. How did these hurdles impact corporate security strategies and initiatives? What are the main challenges security leaders face moving forward?

We asked hundreds of IT and security leaders in an Insight-commissioned IDG survey. Here’s what we learned:

**Cybersecurity at a Crossroads:**

**The Insight 2021 Report**

As a result of increasingly complex IT environments, security teams have been tasked with addressing new vulnerabilities and evolving risks in their environments. Companies shifted cybersecurity modernization priorities in response to challenges presented by the pandemic, focusing on closing security gaps caused by a rapid move to work-from-home environments.

Although most companies completed a number of short-range, block-and-tackle initiatives, security confidence remains low — likely due to teams lacking the resources for executing a wider range of foundational and long-term security efforts.

Organizations made enormous strides to address gaps and reduce cybersecurity risks against new challenges in 2020. But bolstering security postures is a complex and continual effort requiring varied and specialized resources. From strategic planning to day-to-day managed security, we’re here to help you minimize risk, maximize your resources, and make every challenge a step toward stronger defenses.

Security leaders suffer from a lack of resources.

- Lack of automation
- Outdated network access control solutions
- Legacy infrastructure and tools
- Lack of skilled cybersecurity staff

Security awareness and budgets have grown.

- 67% are seeking assistance in developing an overall IT security strategy
- 42% are looking to modernize security operations
- 41% plan to begin or resume staff expansion

Organizations need skilled resources and strategic support.

Looking to the future, organizations plan to spend some of their increased cybersecurity budgets on expanding security teams, modernizing operations, and engaging with outside specialists for strategic support.

- Only 27% of respondents expanded security staff in 2020.
- Only 57% of businesses conducted a data security risk assessment.

The key challenges security teams face in strengthening security postures:

- Lack of automation: 55%
- Outdated network access control solutions: 37%
- Legacy infrastructure and tools: 45%
- Lack of skilled cybersecurity staff: 45%